Policy Title: Technology Incident Reporting Policy	**Policy Number:**
Date Issued: June 10, 2020	**Responsible Executive: Associate Vice President, CIO & CISO**
Date Last Revised: February 1, 2024	**Responsible Office: Information Technology Services**

Technology Incident Reporting Policy

Policy Statement

This policy addresses how the Baylor University ("Baylor" or the "University") community reports a technology-related incident to Information Technology Services ("ITS").

Reason for the Policy

This policy sets forth how to report incidents affecting Baylor technology.

Individuals/Entities Affected by this Policy

Who is affected by this policy

This policy applies to all active members of the University community, including faculty, staff, students, vendors, and affiliates, and to authorized visitors, guests, and others for whom a University technology resource or access to the network has been provided.

Technology affected by this policy

Baylor University technology systems (including, but not limited to, computers, computer accounts, internet, printers, networks, network devices, software, electronic mail ("email"), webpages, video systems, telephones, mobile devices, and telephone long distance and voice mail accounts) are provided for the use of the University community in support of the programs of the University.

Exclusions

NONE

Related Documents and Forms

University Policies and Documents

BU-PP 023 – Standards of Personal Conduct
BU-PP 025 – Technology Usage Policy
BU-PP 029 – Handling of Confidential Information
BU-PP 705 – Faculty Dismissal Policy
BU-PP 807 – Staff Disciplinary Actions
Controlled Unclassified Information Policy
Information Use Policy
Payment Card Industry Policy
Student Disciplinary Procedure
Privacy Policy
Video Surveillance Policy
Website and Email Privacy Statement

Other Documents

- Family Educational Rights and Privacy Act (FERPA) 20 USC §1232g and 34 CFR Part 99
- Health Insurance Portability and Accountability Act (HIPAA) 42 USC §300gg and 1320d; 29 USC §1181 and 45 CFR Parts 146160, 162 and 164
- Gramm-Leach-Bliley Act 15 USC §6801 et seq and 16 CFR Part 313 et seq
- Fair and Accurate Credit Transactions Act (Red Flags Rule) 15 USC §1601 et seq
- Protection of Human Subjects Regulations ("Common Rule") 45 CFR Part 46
- Texas Business and Commerce Code privacy laws Tex. Bus. & Comm. Code Chapters 501-503
- Texas Health & Safety Code Chapter 181 ("HB 300")
- Privacy Act of 1974 5 USC §552a et seq
- Texas Public Information Act Texas Government Code Chapter 552
- Children's Online Privacy Protection Act (COPPA) 15 USC §6501 et seq and 16 CFR Part 312
- European Union General Data Protection Regulation (EU GDPR) EU 2016/679
- PCI DSS
- National Institute of Standards and Technology (NIST) 800-171
- 32 CFR 2002 Control Unclassified Information Final Rule
- DFARs 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting

Definitions

These definitions apply to terms as they are used in this policy.

Baylor University Technology Systems	Baylor-owned, -licensed, or -operated technology systems including, but not limited to, computers, computer accounts, internet, cloud systems, printers, networks, network devices, software, electronic mail ("email"), webpages, video systems, telephones, mobile devices, and telephone long distance and voice mail accounts that are provided for the use of University community in support of the programs of the University
ITS	Information Technology Services
Unauthorized Access	Any action or attempt to utilize, alter, or degrade a Baylor-owned or -operated technology in a manner inconsistent with intended use or university policy
University Community	Faculty, staff, students, affiliates, authorized visitors, guests, and others for whom a University technology resource or access to the network has been provided
Controlled Unclassified Information (CUI)	CUI is government created or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations, and government wide policies.

Personally Identifiable Information (PII)	PII is data that could be used to identify a specific individual.
Confidential Information	Examples of "Confidential Information" include, but are not limited to: student grades, financial aid information, social security numbers, driver's license, payroll and personnel records, personally identifiable information, health information, credit card information, intellectual properties, research data, and passwords. "Confidential Information" includes information in any form, such as paper documents and electronic data.
Family Educational Rights and Privacy Act (FERPA)	Education records that identify students. Examples of FERPA data include, but are not limited to grades, transcripts, class listing, health records and student financial information.
Health Insurance Portability and Accountability Act (HIPAA)	Non-student health information that relates to the past, present or future health of an individual.
European Union General Data Protection Regulation (EU GDPR)	EU GDPR places additional obligations on organizations that control or process personally identifiable information about persons from Europe.

Contacts

Subject	Contact	Telephone	Office email/web site
Policy Management	Information Technology Services	254-710-2711	https://its.web.baylor.edu
Help Desk	Help Desk	254-710-4357	helpdesk@baylor.edu
Baylor University Department of Public Safety	Director of Technical Security	254-710-6617	https://dps.web.baylor.edu
Cybersecurity	Cybersecurity	254-709-5699 254-744-0212	abuse@baylor.edu
Privacy-Related Incident	Office of General Counsel/Chief Privacy Officer	254-710-1360	https://ogc.web.baylor.edu

Responsibilities

ITS Chief Information Security Officer or Designee	Responsible for developing and implementing an information security program to ensure that University communications, systems, and assets are safeguarded from threats
Chief Information Officer or Designee	Responsible for ensuring the policy remains current and for managing the application of the policy
Chief Privacy Officer	Responsible for providing support and guidance in the event of a privacy-related incident

Principles

Reporting a Technology Security Incident

ITS staff should be notified immediately of any suspected or confirmed security incident involving Baylor University technology. If it is unclear as to whether a situation should be considered a security incident, ITS should be contacted to evaluate the situation.

A security incident meets one or more of the following conditions:

- Any potential violation of federal law, Texas law, or Baylor University policy involving Baylor University information technology assets.
- A breach, attempted breach, or other unauthorized access of a Baylor University information technology and data. The incident may originate from within the Baylor University network or an outside entity.
- Any Internet worms, viruses, or malware.
- Any conduct using in whole or in part Baylor University information technology which could be construed as harassing, or in violation of Baylor University policies.

When a security incident is suspected, please take the following actions:

- If the incident involves a compromised University computer
    - Do not turn off the computer or close any of the programs.
    - Do not restart the computer.
    - Immediately disconnect the computer from the network by removing the network cable from the back of the computer.
    - If the computer is connected to the network wirelessly, disconnect the wireless network. If you need assistance, call the Help Desk.
    - Click here for instructions on disconnecting your computer from the network.
- Report the security incident details including date and time, nature of the incident, any additional information that may aid in responding to the incident in a prompt manner.
- When a cyber incident affects FERPA, HIPAA, EU GDPR, CUI, personally identifiable or confidential information immediately report the incident to ITS Security.

Baylor University Department of Public Safety

Any security incident involving possible violations of federal or state law should be immediately reported to the Baylor University Department of Public Safety (“BUDPS”). BUDPS will work with ITS security staff and other law enforcement agencies as necessary to resolve the incident.

Director of Technical Security: 254-710-6617

Baylor Police: 254-710-2222

Help Desk

Incidents can be reported to the help desk. The help desk hours are Monday – Friday from 8:00 am to 5:00 pm, excluding holidays.

Phone: 254-710-4357 (help)

Email: helpdesk@baylor.edu

ITS Security

Any other security incidents should be immediately reported to Baylor University ITS security staff. ITS security staff will then take the appropriate response.

Email: abuse@baylor.edu

Chief Information Security Officer: 254-709-5699

Director of Cyber Security Operations: 254-749-5951

Disclaimer

The latest official copy of this policy is available from the Information Technology Services and the Human Resources websites. Copies will also be posted on various University servers, such as the Baylor Web server. Other standards and guidelines (for electronic mail, webpages, newsgroups, copyright, directory information, etc.) may be found on the Baylor Web server at: **https://its.web.baylor.edu/policies.**